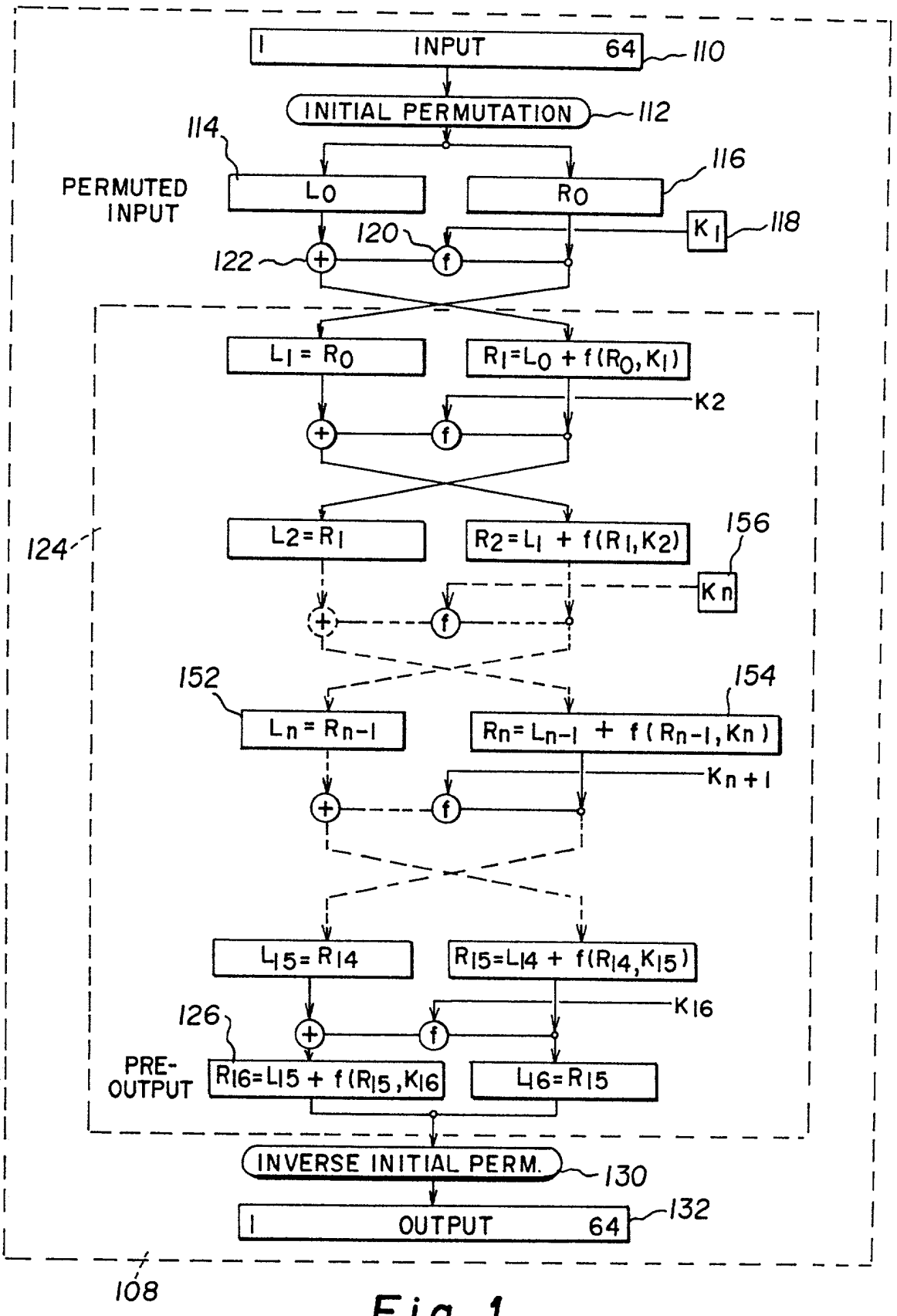
INPUT 64
110
INITIAL PERMUTATION
112
114
116
PERMUTED INPUT
L0
R0
K1
118
120
122
L1 = R0
R1=L0 + f(R0, K1)
K2
124
L2=R1
R2=L1 + f(R1,K2)
156
Kn
152
154
Ln = Rn-1
Rn= Ln-1 + f(Rn-1, Kn)
Kn+1
L15= R14
R15=L14 + f(R14,K15)
K16
126
PRE-OUTPUT
R16=L15 + f(R15,K16)
L16=R15
INVERSE INITIAL PERM.
130
OUTPUT 64
132
108

Fig. 1

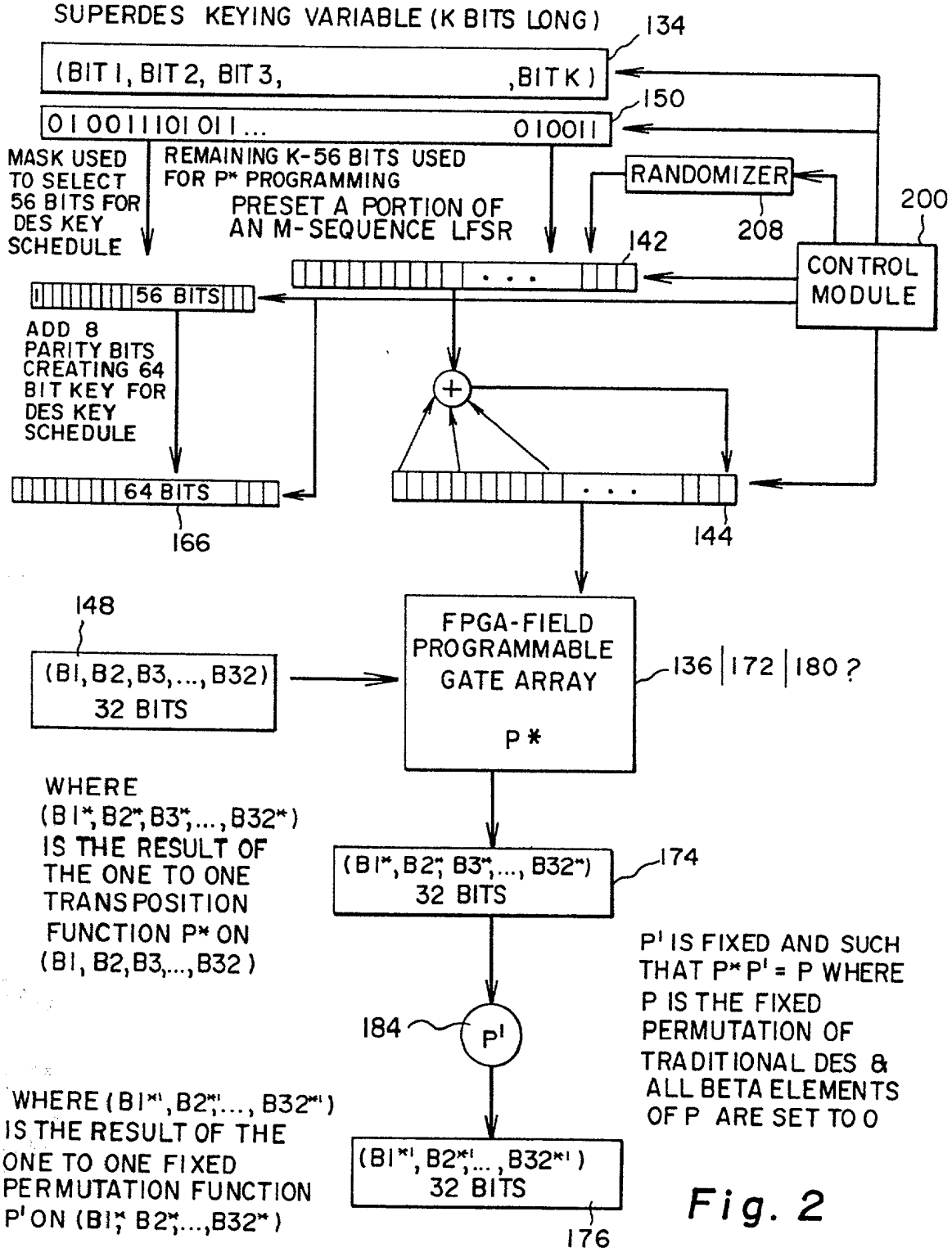
SUPERDES KEYING VARIABLE (K BITS LONG)
134
(BIT 1, BIT 2, BIT 3, ,BIT K)
150
0 1 0 0 1 1 1 0 1 0 1 1 ... 0 1 0 0 1 1
MASK USED TO SELECT 56 BITS FOR DES KEY SCHEDULE
REMAINING K-56 BITS USED FOR P* PROGRAMMING
PRESET A PORTION OF AN M-SEQUENCE LFSR
RANDOMIZER
208
200
142
CONTROL MODULE
56 BITS
ADD 8 PARITY BITS CREATING 64 BIT KEY FOR DES KEY SCHEDULE
64 BITS
166
144
148
(B1, B2, B3, ..., B32)
32 BITS
FPGA-FIELD PROGRAMMABLE GATE ARRAY
P*
136 | 172 | 180 ?
WHERE (B1*, B2*, B3*, ..., B32*) IS THE RESULT OF THE ONE TO ONE TRANSPOSITION FUNCTION P* ON (B1, B2, B3, ..., B32)
(B1*, B2*, B3*, ..., B32*)
32 BITS
174
184
P'
P' IS FIXED AND SUCH THAT P* P' = P WHERE P IS THE FIXED PERMUTATION OF TRADITIONAL DES & ALL BETA ELEMENTS OF P ARE SET TO 0
WHERE (B1*', B2*', ..., B32*') IS THE RESULT OF THE ONE TO ONE FIXED PERMUTATION FUNCTION P' ON (B1*, B2*, ..., B32*)
(B1*', B2*', ..., B32*')
32 BITS
176

Fig. 2

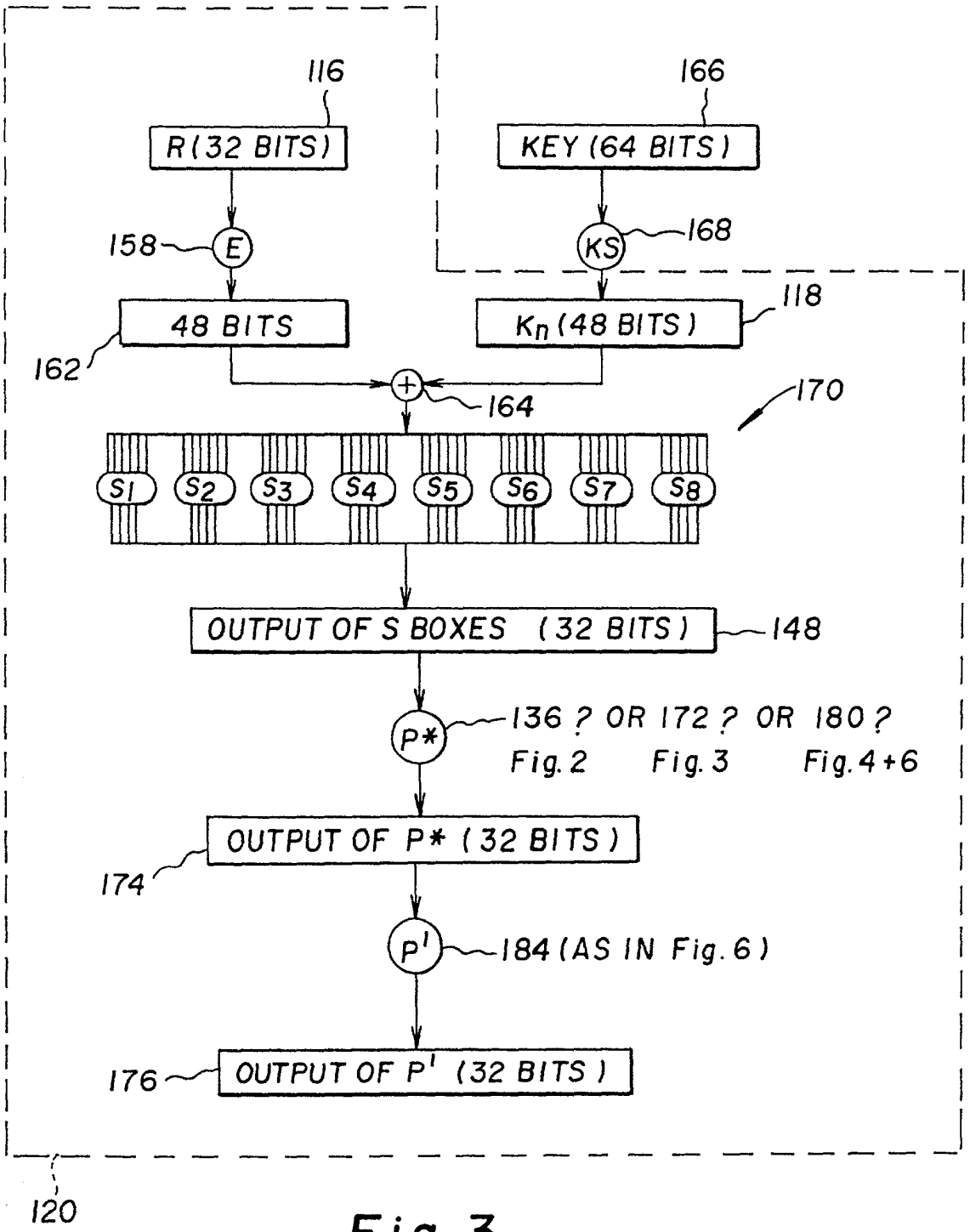

Fig. 3

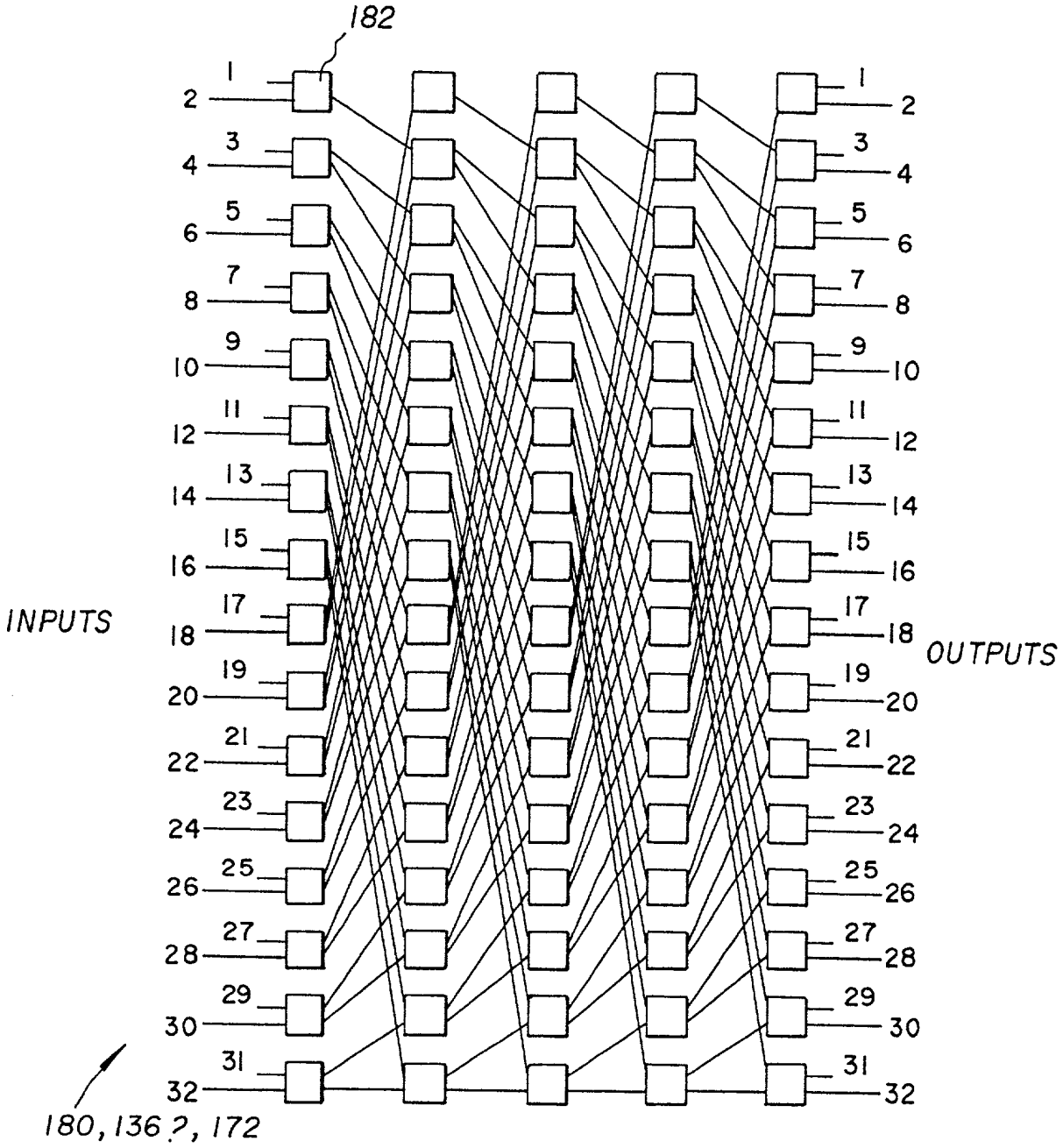
182
INPUTS
OUTPUTS
180, 136?, 172
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

Fig. 4

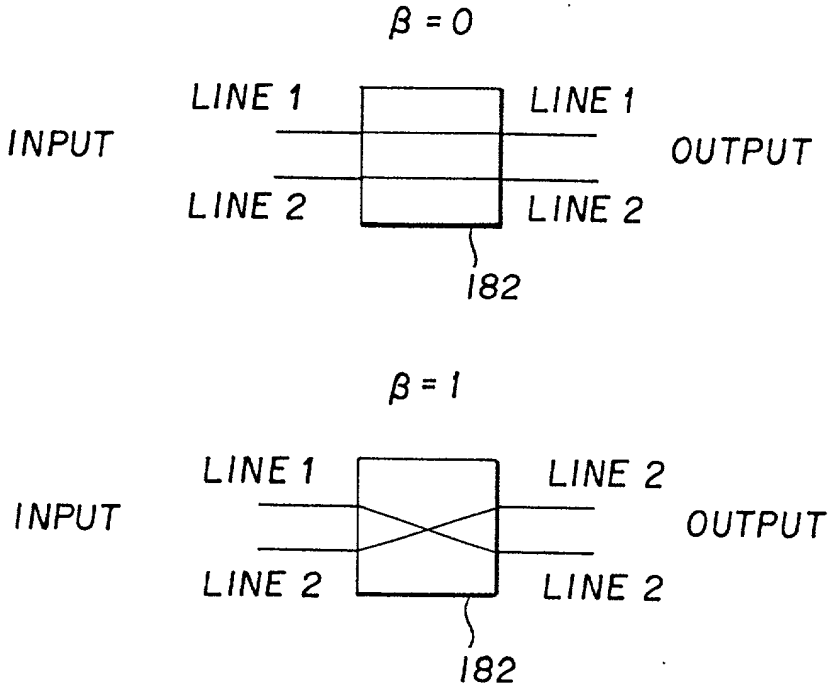
β = 0
LINE 1
LINE 1
INPUT
OUTPUT
LINE 2
LINE 2
182
β = 1
LINE 1
LINE 2
INPUT
OUTPUT
LINE 2
LINE 2
182

Fig. 5

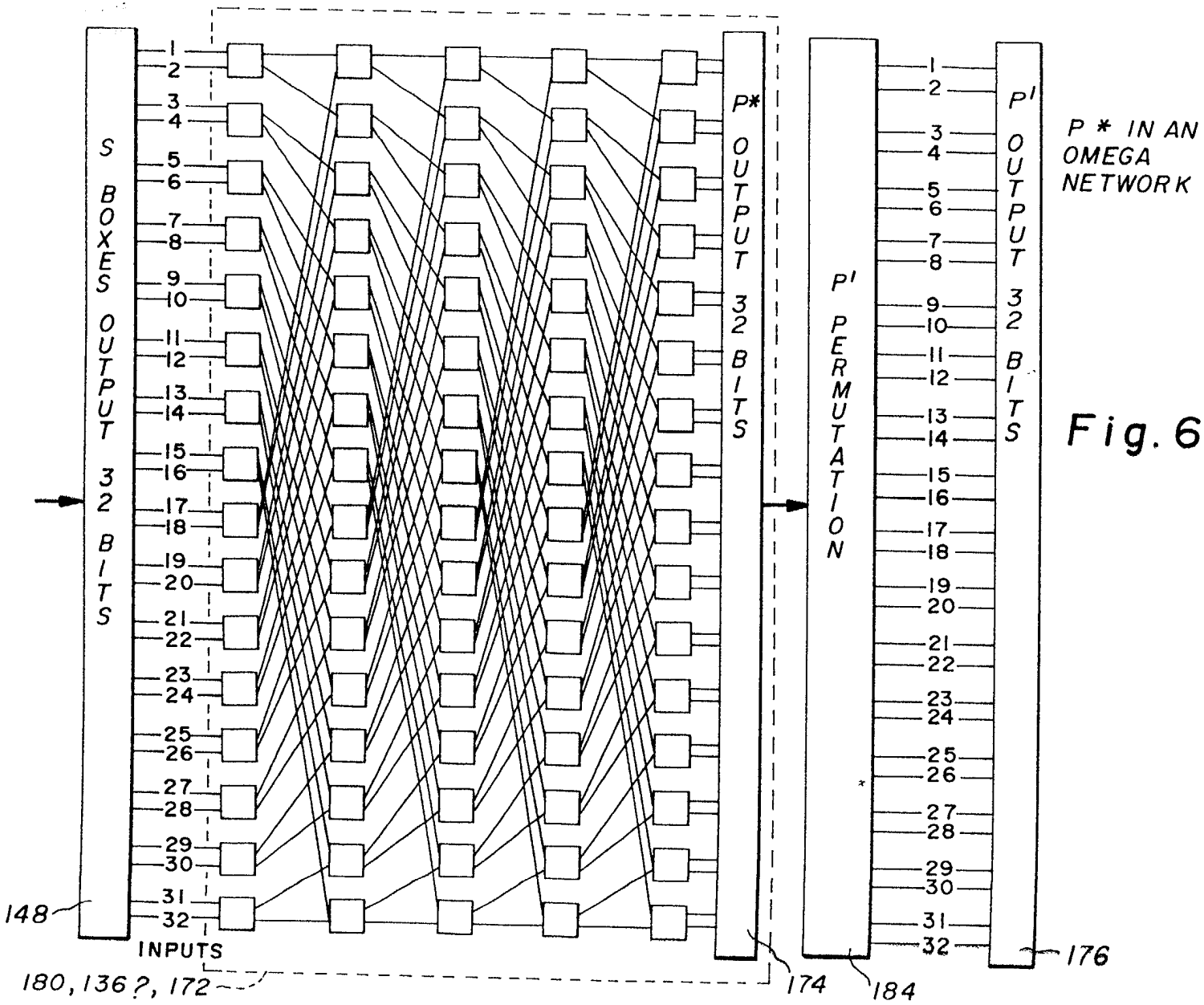

Fig. 6

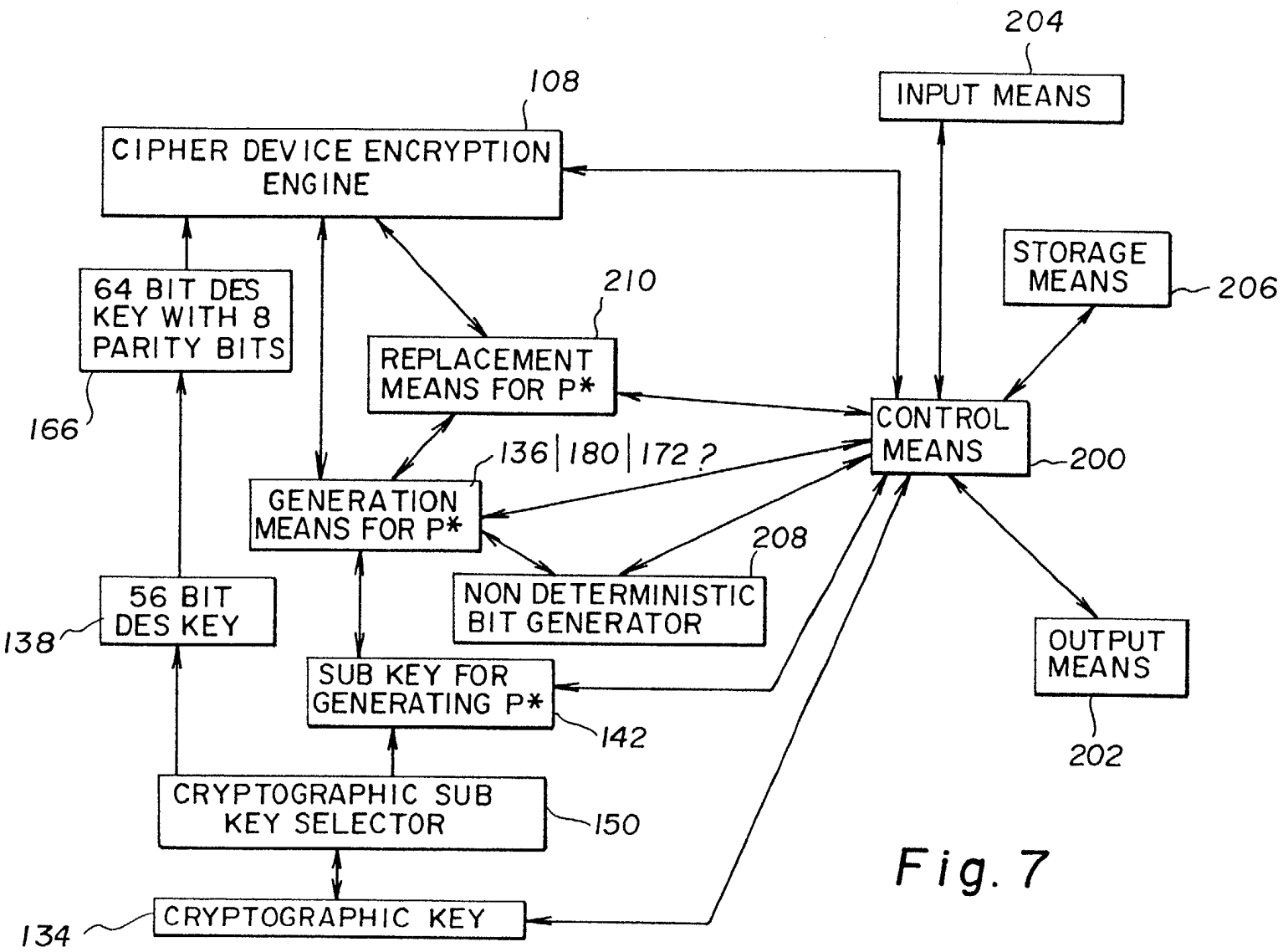

Fig. 7

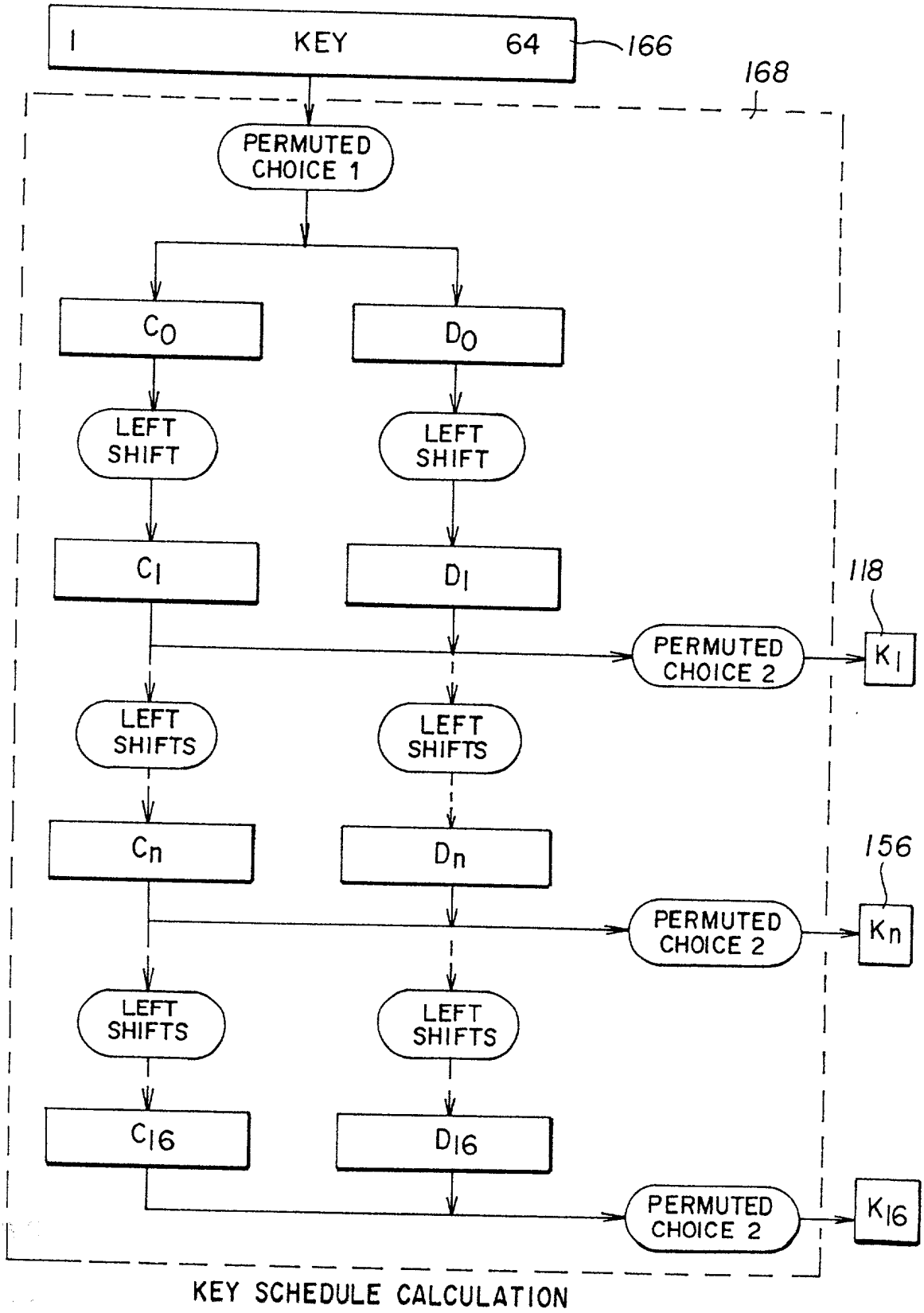
1
KEY
64
166
168
PERMUTED CHOICE 1
C_0
D_0
LEFT SHIFT
LEFT SHIFT
C_1
D_1
118
PERMUTED CHOICE 2
K_1
LEFT SHIFTS
LEFT SHIFTS
C_n
D_n
156
PERMUTED CHOICE 2
K_n
LEFT SHIFTS
LEFT SHIFTS
C_{16}
D_{16}
PERMUTED CHOICE 2
K_{16}
KEY SCHEDULE CALCULATION

Fig. 8